AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes changes to Figure 5A. This sheet, which includes Figures 5A and 5B, replaces the original sheet including Figures 5A and 5B.

Attachment: Replacement Sheet

Annotated Sheet Showing Changes

REMARKS

These remarks and the accompanying claim amendments are responsive to the Office

Action dated July 12, 2005, having a shortened period for response that expires October 12, 2005

(hereinafter referred to as "the Office Action"). Claims 1-17 were pending at the time of the last

examination, and each stands rejected. By this response, Claims 1, 3-6, 8-10, 12, 13 and 15-17

are cancelled, leaving only Claims 2, 7, 11 and 14 remaining. Each of the remaining Claims 2, 7,

11 and 14 are currently amended herein and are in independent form.

The Office Action rejects Claims 1, 4-6, 8-17 under 35 U.S.C. 102(b) as being

anticipated by United States patent number 4,159,468 issued to Barnes et al. (hereinafter referred

to as "Barnes"). This rejection is moot with respect to cancelled Claims 1, 4-6, 8-10, 12, 13 and

15-17, but remains with respect to Claims 11 and 14. Furthermore, the Office Action rejects

Claims 2, 3 and 7 under 35 U.S.C. 103(a) as being unpatentable over Barnes in view of United

States patent number 6,021,199 issued to Ishibashi (hereinafter referred to as "Ishibashi"). The

rejection is moot with respect to cancelled Claim 3, but remains with respect to Claims 2 and 7.

Summary of Barnes

Barnes discloses apparatus extracting information from the header of a received packet,

deciding if the information extracted is stored in a key list, and encrypting/decrypting the packet

according to the decision. In the encryption process of Barnes, a device can be made sensitive to

control sequences which place the device in an out of an encryption mode. The control

sequences can be entered between the start (STX) and end (ETX) of the message. Hence, the

device can encrypt selected portions of the message and leave other portions to be transmitted in

plain text.

However, each object of Barnes is different from that of present invention. The object of Barnes is to provide transparent and secure communications between computer systems or LANs connected to an open network. On the other hand, the object of the present invention is to prevent a cryptographic key or authentication key from being broken.

For example, when a short packet section is intruded, it will be easily broken. In the present invention, a bit stream with a small number of bits or a bit stream that can be cryptanalyzed easily is not encrypted as recited in Claims 2 and 11. The same is equally true of the invention recited in Claims 7 and 14, in which the type of the bit stream is determined by the number of bits or a degree of effect of tampering.

As discussed above, the purpose of the present invention is never disclosed in Barnes. Also, no one or ordinary skill in the art would not think of the selective encryption and authentication as recited in Claims 2, 7, 11 and 14, even in light of Barnes and Ishibashi. Therefore, the 35 U.S.C. 102(b) ad 103(a) rejections of the claims should be withdrawn.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 12th day of October, 2005.

Respectfully submitted,

ADRIAN J. LEE
Registration No. 42,785
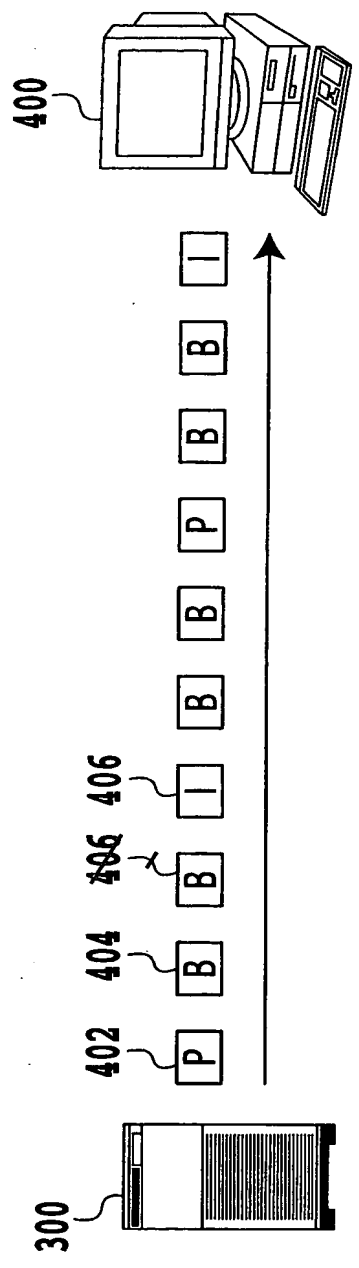Attorney for Applicant
Customer No. 022913

AJL:ds
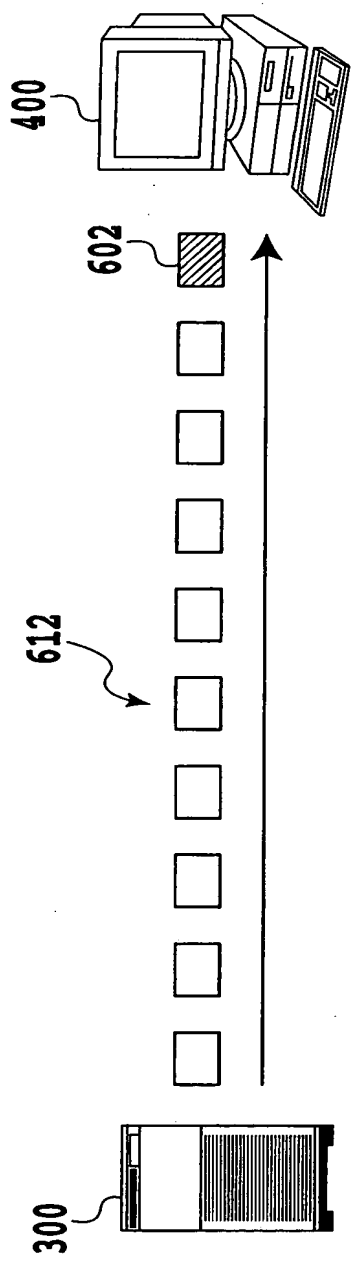DS0000004148V001

FIG.5A

300

402 404 *406 406
P B B I B B B P B B B I

400

FIG.5B

300

612

602

400